大型网络中使用 Mysql 和 IIS 部署
ESET NOD32 企业版

二版科技（深圳）有限公司

Exclusively Distributed by Version 2 Limited

目　　录

第一章　系统需求 3

第二章　安装 Mysql 数据库 4

1. 安装 MySql 数据库 4

2. 安装 MySql ODBC 数据源 8

第三章　安装远程管理控制台 9

1. 按装 era_server_nt32_chs.msi 9

2. 安装 era_console_nt32_chs.msi 14

第三章　定制客户端安装包 16

1. 制作客户端配置文件 16

2. 打包客户端 20

第四章　服务器防病毒软件安装 24

第五章　使用 IIS 架设本地更新服务器 25

第六章　IIS 高级功能 31

第七章　服务器自动维护 35

第八章　服务与支持 37

Exclusively Distributed by Version 2 Limited

第一章 系统需求

在大型网络中，数据的交互量非常大，所有客户端的信息，威胁日志、防火墙日志、事件日志、扫描日志、任务等，全部都集中保存到远程管理服务器，所有客户端的更新也指向远程管理服务器，远程管理服务器必将处于一个非常忙碌的状态。为了最大限度地平衡服务器的性能，我们建议在大型网络中使用额外的 Mysql 数据库和 IIS 服务器来部署 ESET NOD32 企业版。

以下是在大型网络中部署 ESET NOD32 企业版的系统配置建议：

硬件需求对照表：

客户端数	CPU	内存	安装硬盘空间	剩余硬盘空间	网卡
<500	>1GHz	1GB	50MB	5GB	100Mb/s
<1000	>2GHz	2GB	50MB	10GB	100Mb/s
>1000<5000	>2GHz 双核	4GB	50MB	20GB	1Gb/s
>5000	>2Ghz 四核	4GB	50MB	30GB(RAID 更佳)	1Gb/s

软件需求：

操作系统	Windows Server 2003（打齐 MS 补丁）
数据库	MySQL
HTTP 服务器	IIS (Windows Server 2003)

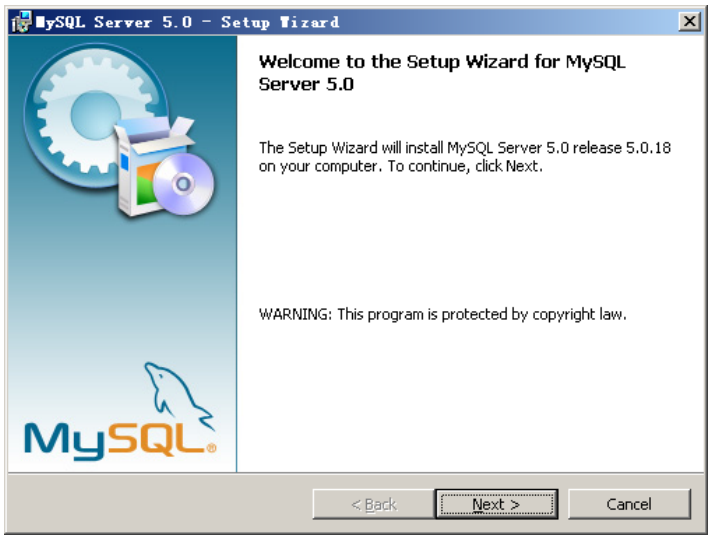
备注：在 Server 上安装 ESET NOD32 防病毒软件之前，请务必将当前机器已安装的杀毒软件完全卸载，并且强烈建议您打齐所有的操作系统补丁（正版验证补丁除外），服务器也按装好 IIS 服务。

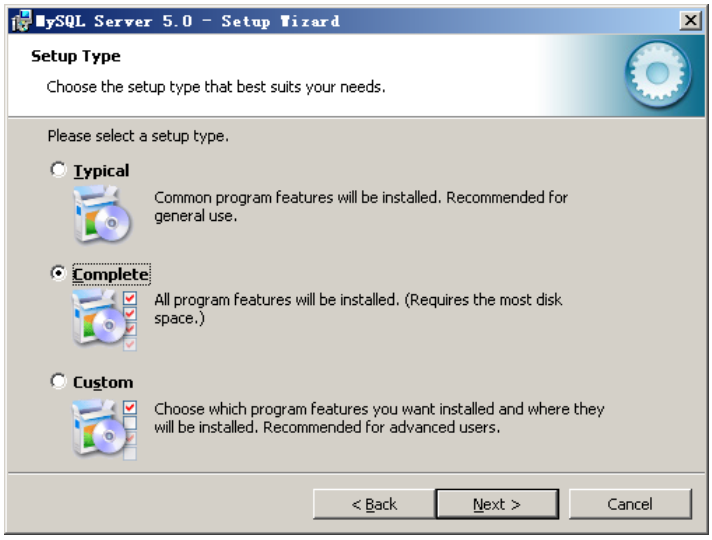
Exclusively Distributed by Version 2 Limited

第二章 安装 Mysql 数据库

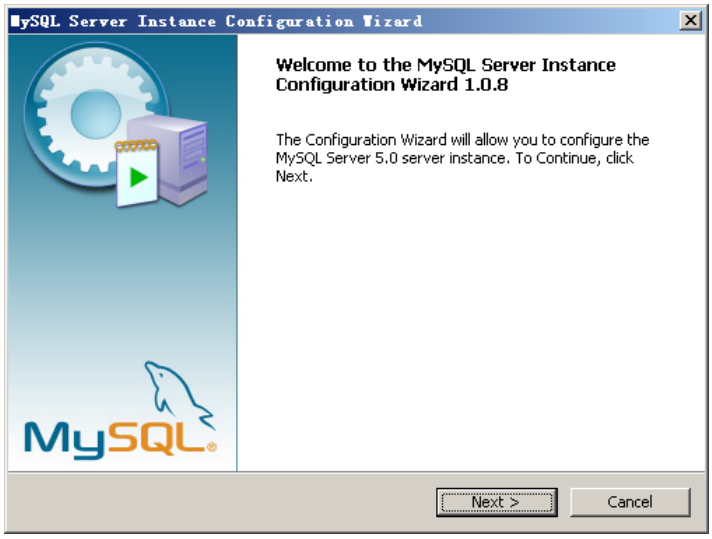
1. 安装 MySql 数据库

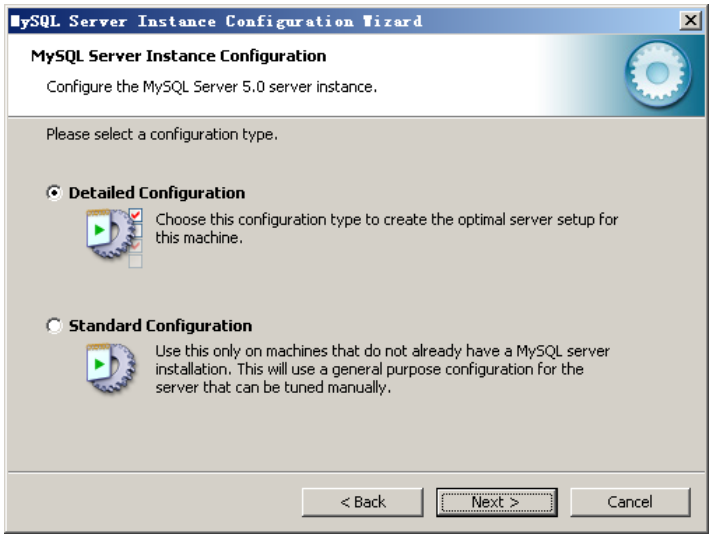
MySql 是完全免费的，可以到起官方网站下载：www.mysql.cn

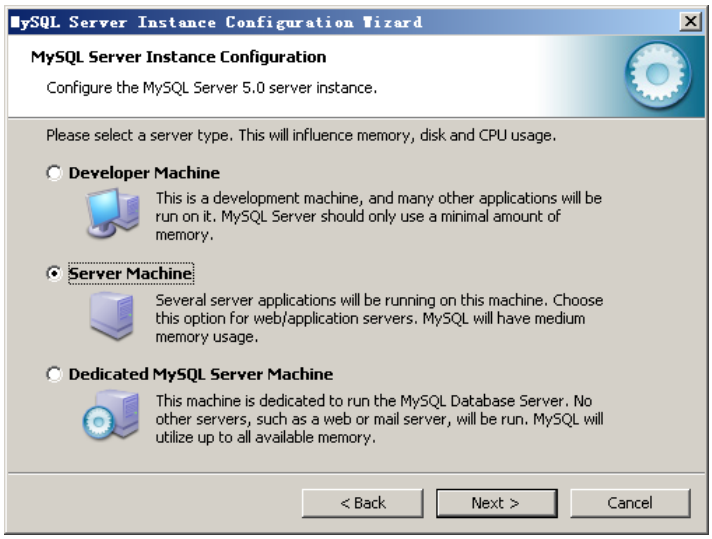

MySQL Server 5.0 - Setup Wizard
Welcome to the Setup Wizard for MySQL Server 5.0
The Setup Wizard will install MySQL Server 5.0 release 5.0.18 on your computer. To continue, click Next.
WARNING: This program is protected by copyright law.
MySQL
< Back
Next >
Cancel


MySQL Server 5.0 - Setup Wizard
Setup Type
Choose the setup type that best suits your needs.
Please select a setup type.
Typical
Common program features will be installed. Recommended for general use.
Complete
All program features will be installed. (Requires the most disk space.)
Custom
Choose which program features you want installed and where they will be installed. Recommended for advanced users.
< Back
Next >
Cancel

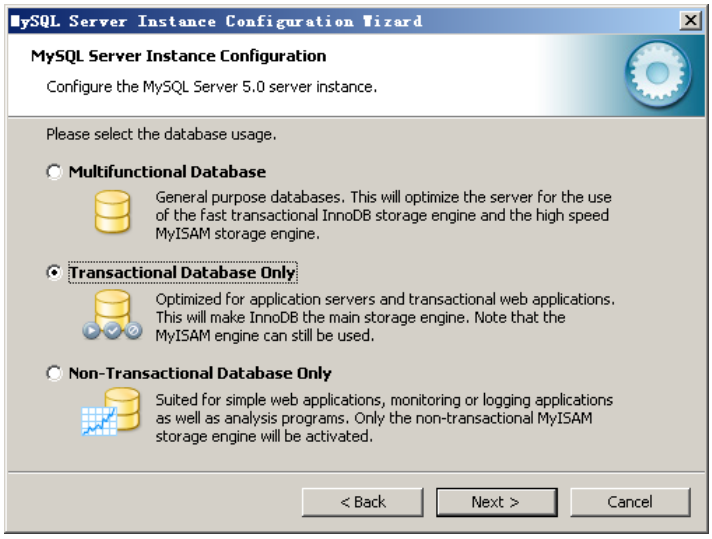
Exclusively Distributed by Version 2 Limited

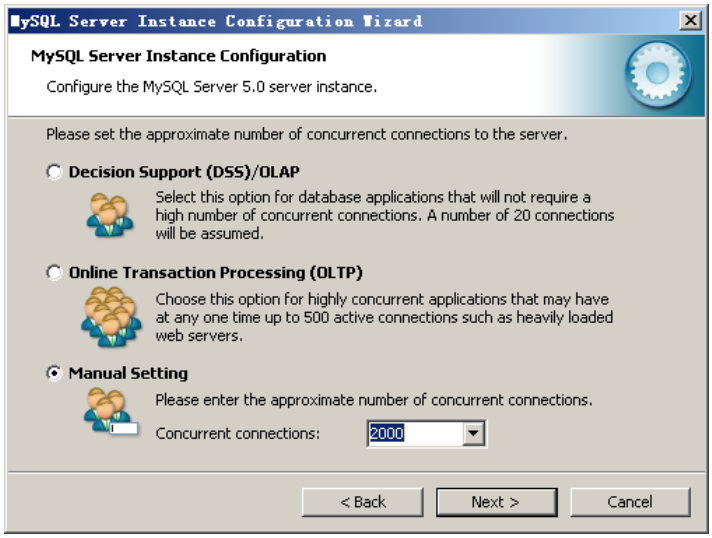

MySQL Server Instance Configuration Wizard
Welcome to the MySQL Server Instance Configuration Wizard 1.0.8
The Configuration Wizard will allow you to configure the MySQL Server 5.0 server instance. To Continue, click Next.
MySQL
Next >
Cancel


MySQL Server Instance Configuration Wizard
MySQL Server Instance Configuration
Configure the MySQL Server 5.0 server instance.
Please select a configuration type.
Detailed Configuration
Choose this configuration type to create the optimal server setup for this machine.
Standard Configuration
Use this only on machines that do not already have a MySQL server installation. This will use a general purpose configuration for the server that can be tuned manually.
< Back
Next >
Cancel

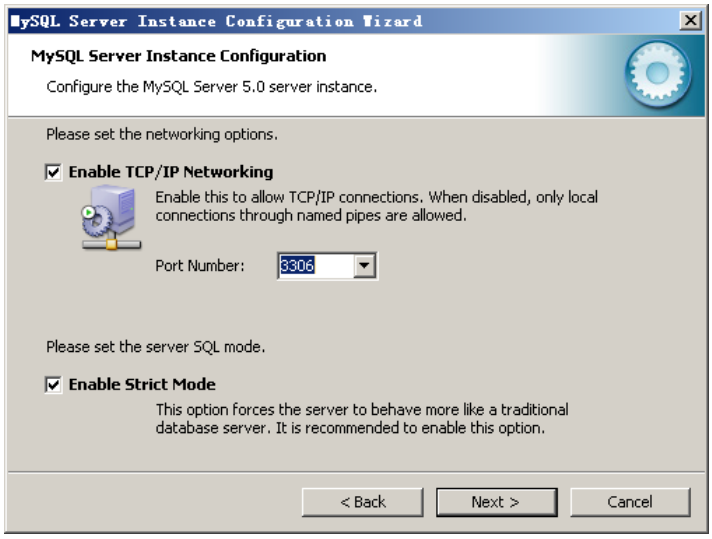

MySQL Server Instance Configuration Wizard
MySQL Server Instance Configuration
Configure the MySQL Server 5.0 server instance.
Please select a server type. This will influence memory, disk and CPU usage.
Developer Machine
This is a development machine, and many other applications will be run on it. MySQL Server should only use a minimal amount of memory.
Server Machine
Several server applications will be running on this machine. Choose this option for web/application servers. MySQL will have medium memory usage.
Dedicated MySQL Server Machine
This machine is dedicated to run the MySQL Database Server. No other servers, such as a web or mail server, will be run. MySQL will utilize up to all available memory.
< Back
Next >
Cancel

Exclusively Distributed by Version 2 Limited





备注：上图中，手工设定的并发量请依据您的实际需要来更改。

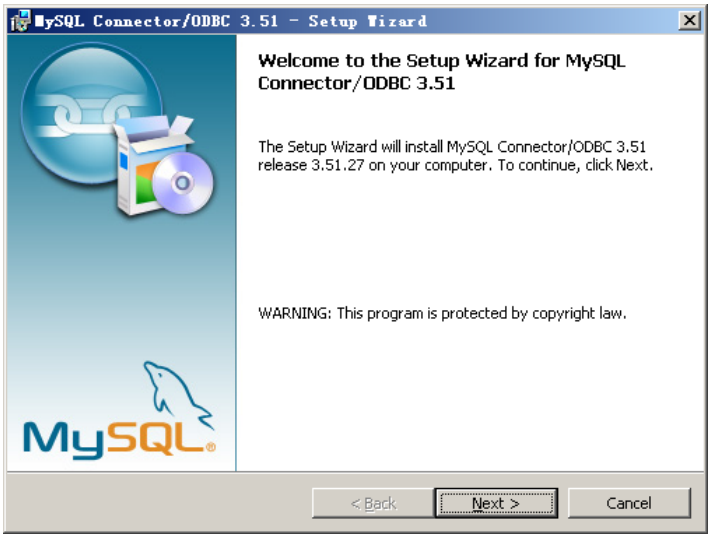

MySQL Server Instance Configuration Wizard
MySQL Server Instance Configuration
Configure the MySQL Server 5.0 server instance.
Please set the networking options.
Enable TCP/IP Networking
Enable this to allow TCP/IP connections. When disabled, only local connections through named pipes are allowed.
Port Number:
3306
Please set the server SQL mode.
Enable Strict Mode
This option forces the server to behave more like a traditional database server. It is recommended to enable this option.
< Back
Next >
Cancel

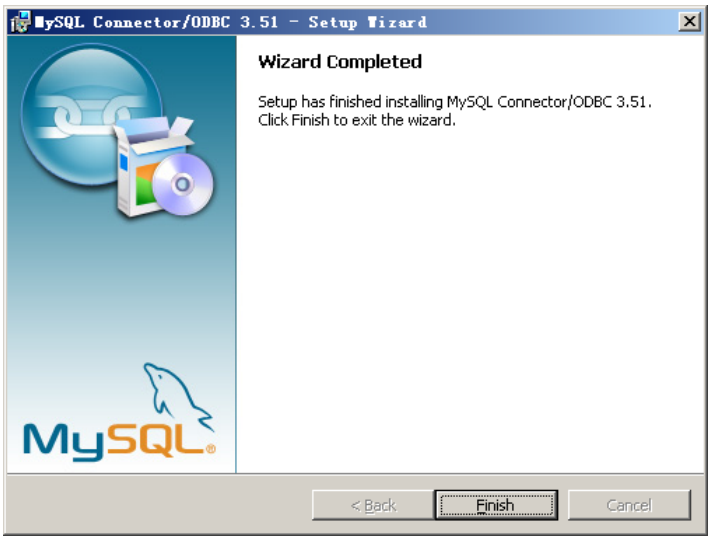
MySQL Server Instance Configuration Wizard
MySQL Server Instance Configuration
Configure the MySQL Server 5.0 server instance.
Please set the security options.
Modify Security Settings
root
New root password:
*****
Enter the root password.
Confirm:
*****
Retype the password.
Enable root access from remote machines
Create An Anonymous Account
This option will create an anonymous account on this server. Please note that this can lead to an insecure system.
< Back
Next >
Cancel

注意记住此时的密码

2. 安装 MySql ODBC 数据源

下载地址：http://skycn.net/soft/2141.html

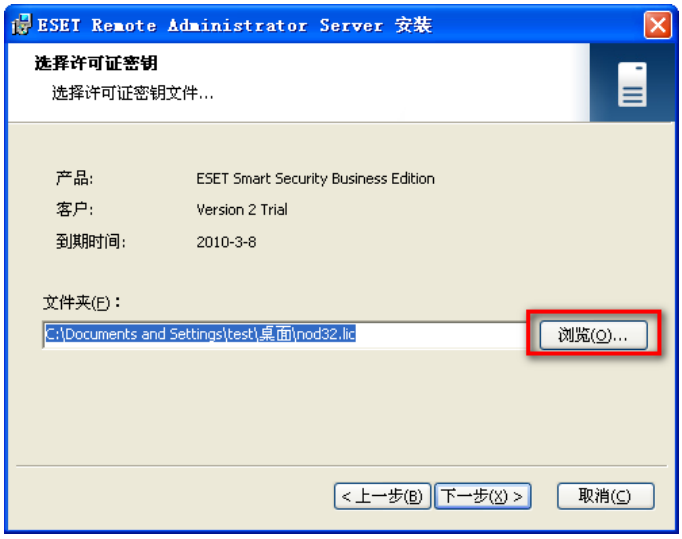

MySQL Connector/ODBC 3.51 - Setup Wizard
Welcome to the Setup Wizard for MySQL Connector/ODBC 3.51
The Setup Wizard will install MySQL Connector/ODBC 3.51 release 3.51.27 on your computer. To continue, click Next.
WARNING: This program is protected by copyright law.
MySQL
< Back
Next >
Cancel

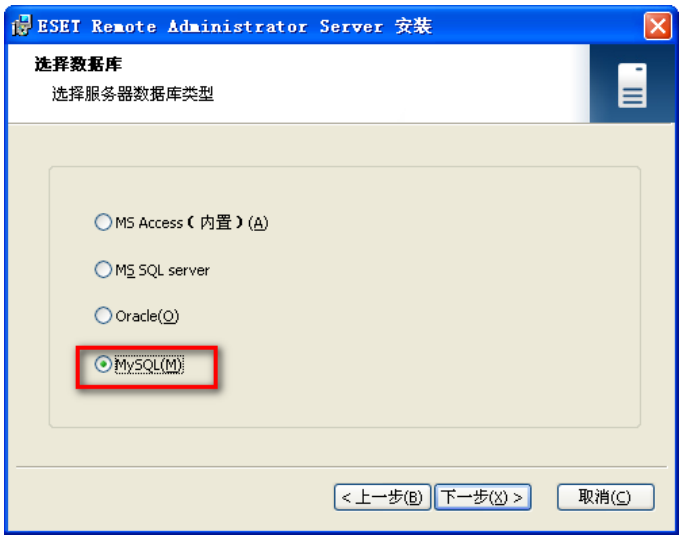


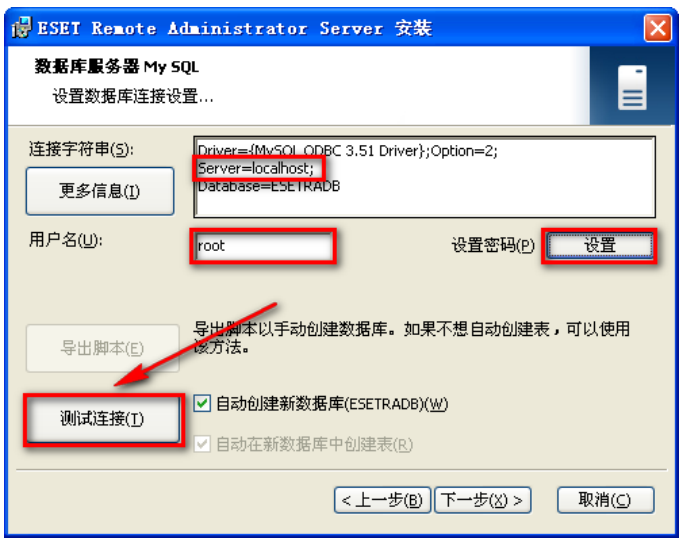
第三章　安装远程管理控制台

打开企业版光盘——远程管理套件

1. 按装 era_server_nt32_chs.msi


ESET Remote Administrator Server 安装
选择许可证密钥
选择许可证密钥文件...
产品:
ESET Smart Security Business Edition
客户:
Version 2 Trial
到期时间:
2010-3-8
文件夹(F):
C:\Documents and Settings\test\桌面\nod32.lic
浏览(O)...
< 上一步(B)
下一步(X) >
取消(C)


ESET Remote Administrator Server 安装
选择数据库
选择服务器数据库类型
MS Access (内置) (A)
MS SQL server
Oracle(O)
MySQL(M)
< 上一步(B)
下一步(X) >
取消(C)

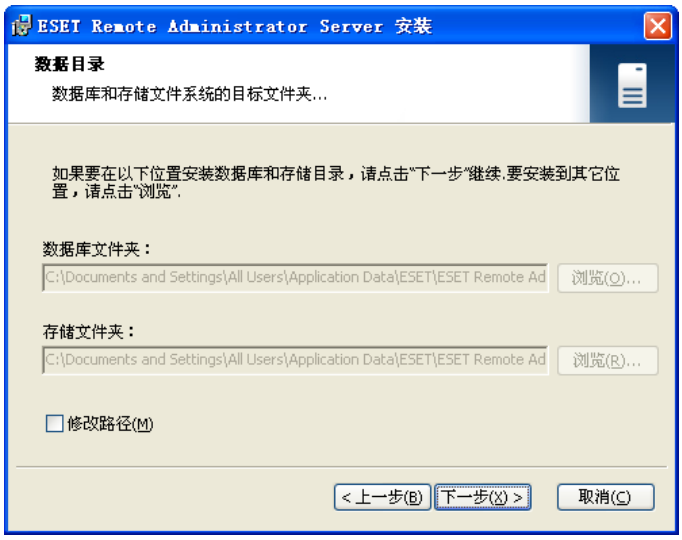

ESET Remote Administrator Server 安装
数据库服务器 My SQL
设置数据库连接设置...
连接字符串(S):
更多信息(I)
Driver={MySQL ODBC 3.51 Driver};Option=2;
Server=localhost;
Database=ESETRADB
用户名(U):
root
设置密码(P)
设置
导出脚本(E)
导出脚本以手动创建数据库。如果不想自动创建表，可以使用该方法。
测试连接(T)
自动创建新数据库(ESETRADB)(W)
自动在新数据库中创建表(R)
< 上一步(B)
下一步(X) >
取消(C)

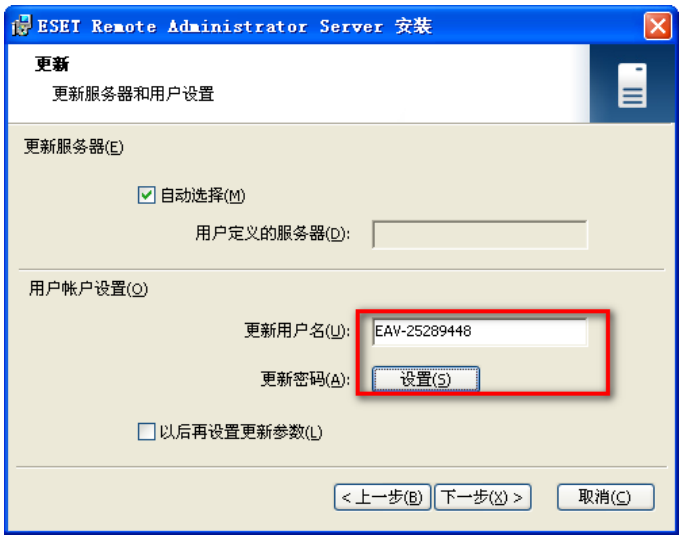
注意：

Server=localhost;

用户名和密码请填写在 Mysql 中安装时设定的用户名和密码

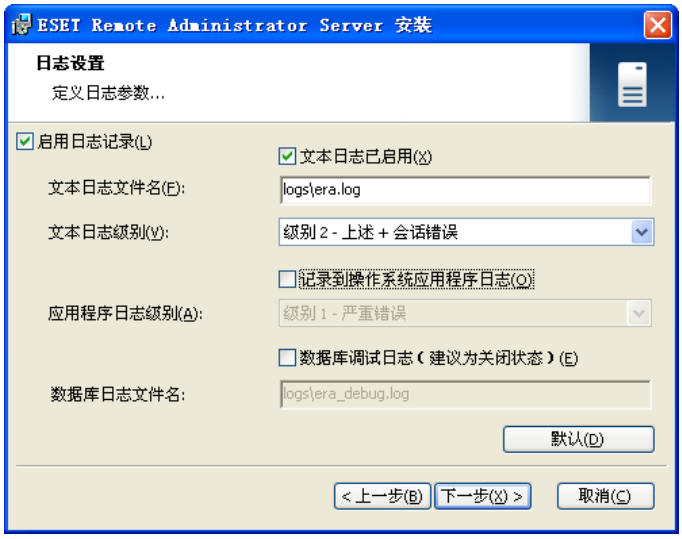
点击测试连接，提示成功即可进行下一步下一步安装。

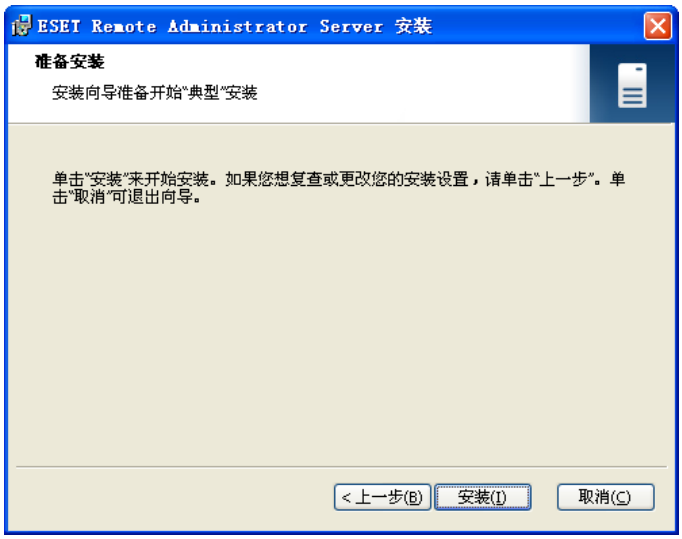


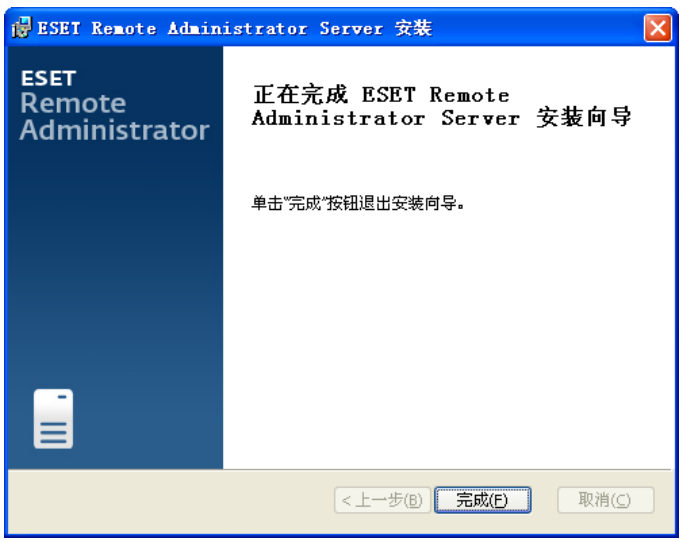


在此输入企业版授权账号密码“更新用户名”、“更新密码”

直接点击下一步继续。

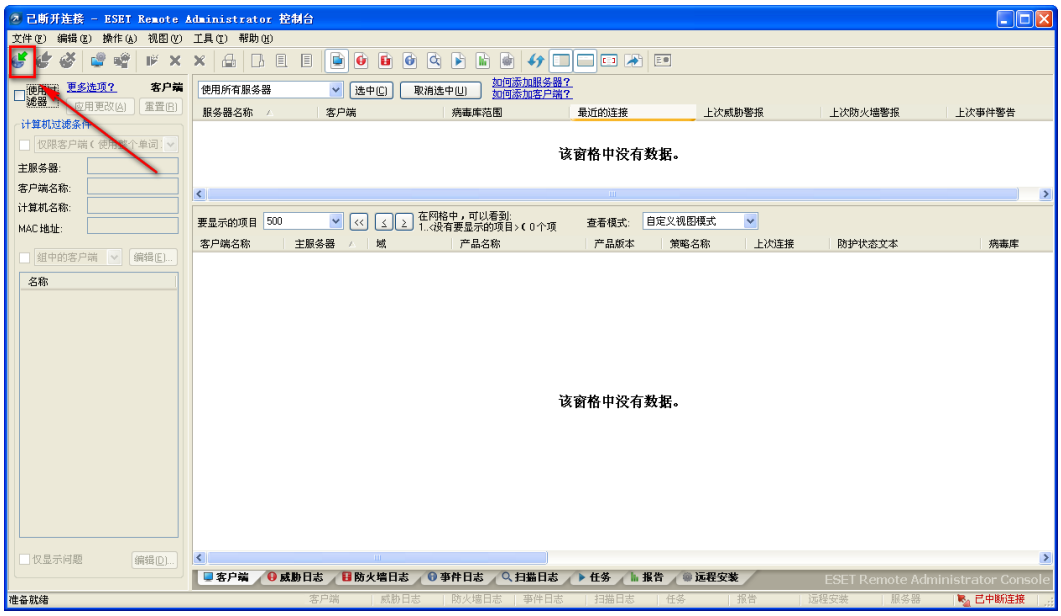


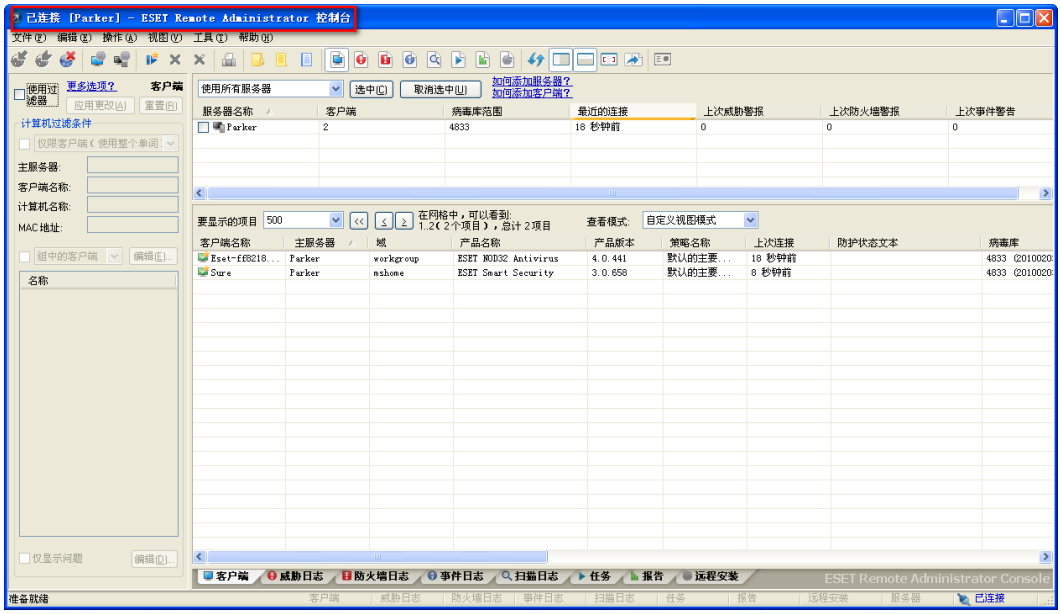




Exclusively Distributed by Version 2 Limited

2. 安装 era_console_nt32_chs.msi





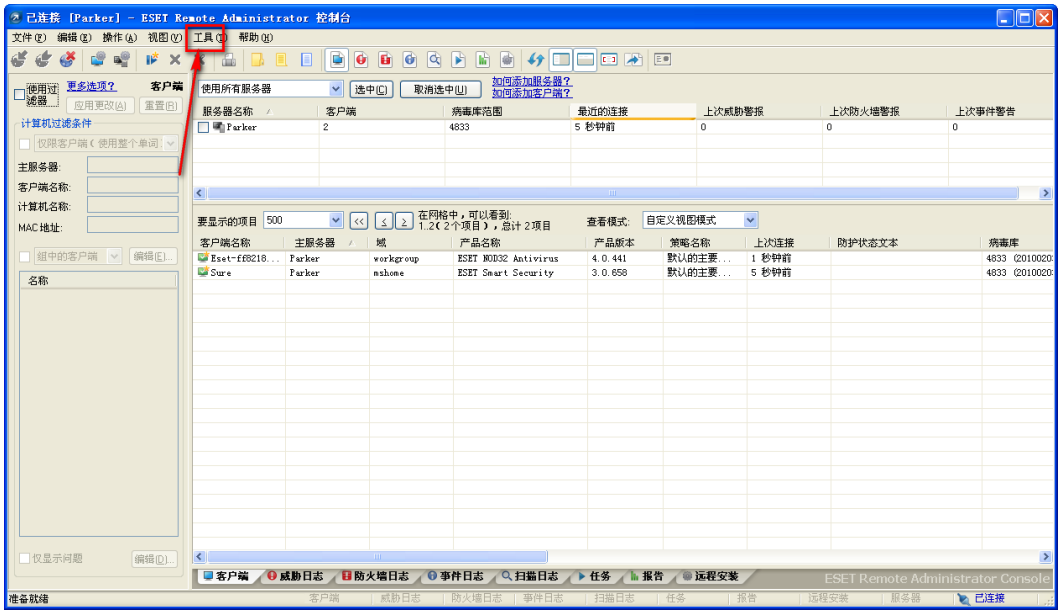
Exclusively Distributed by Version 2 Limited

第三章 定制客户端安装包

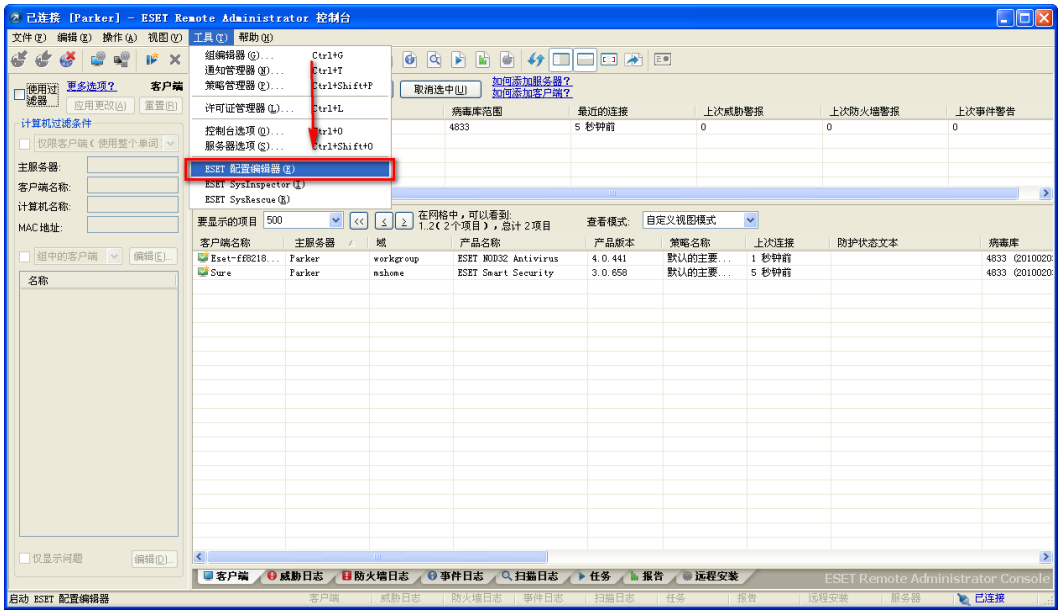
由于 ESTT NOD32 客户端原始安装程序是类似 eavbe_nt32_chs.msi(防病毒软件企业版)/essbe_nt32_chs.msi(安全套装企业版)，若采用默认配置，安装完毕之后，在管理控制台中无法看到客户端，客户端在安装时也需要输入企业版账号密码，将连接到互联网更新病毒库。所以需要对其进行配置，做一个定制好的客户端安装包：客户端安装完毕后将自动连接到企业内部的 ESET NOD32 服务器升级病毒库，并自动纳入远程管理。

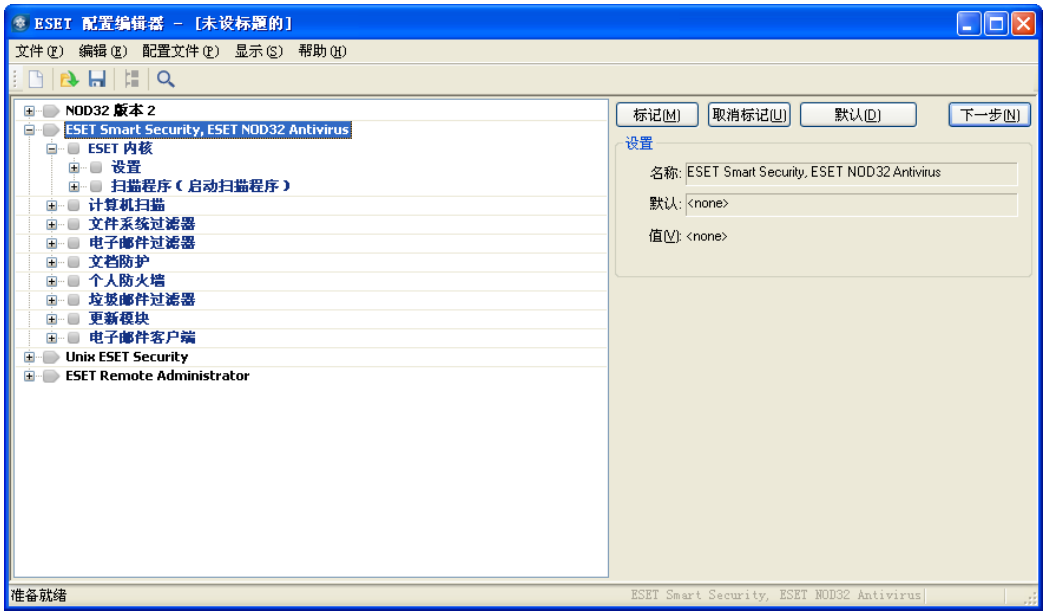
下面是手工定制客户端安装包的详细步骤：

1. 制作客户端配置文件

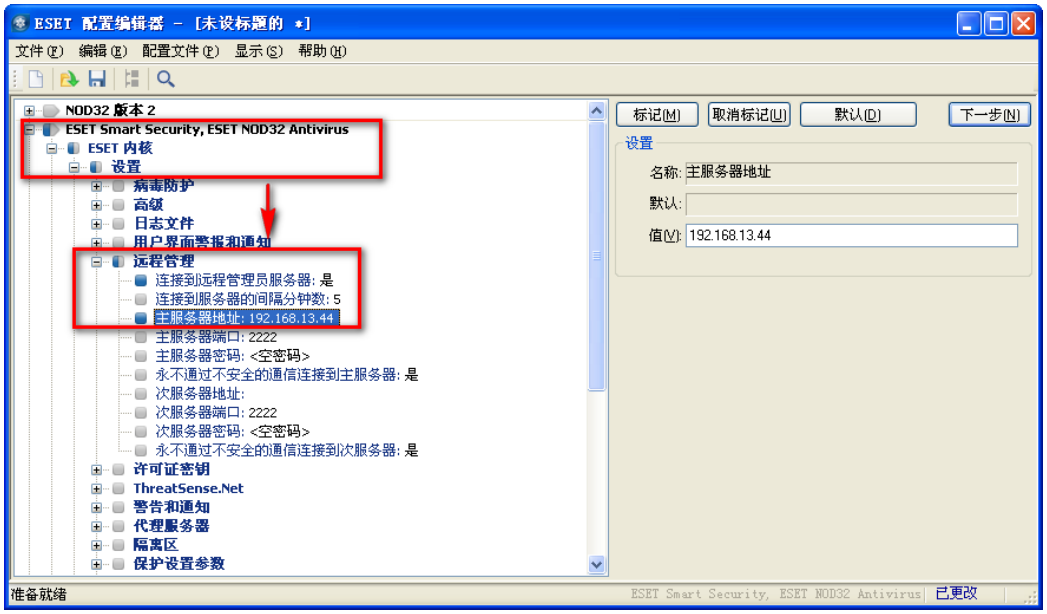


Version 2 二版 www.version-2.com
Exclusively Distributed by Version 2 Limited



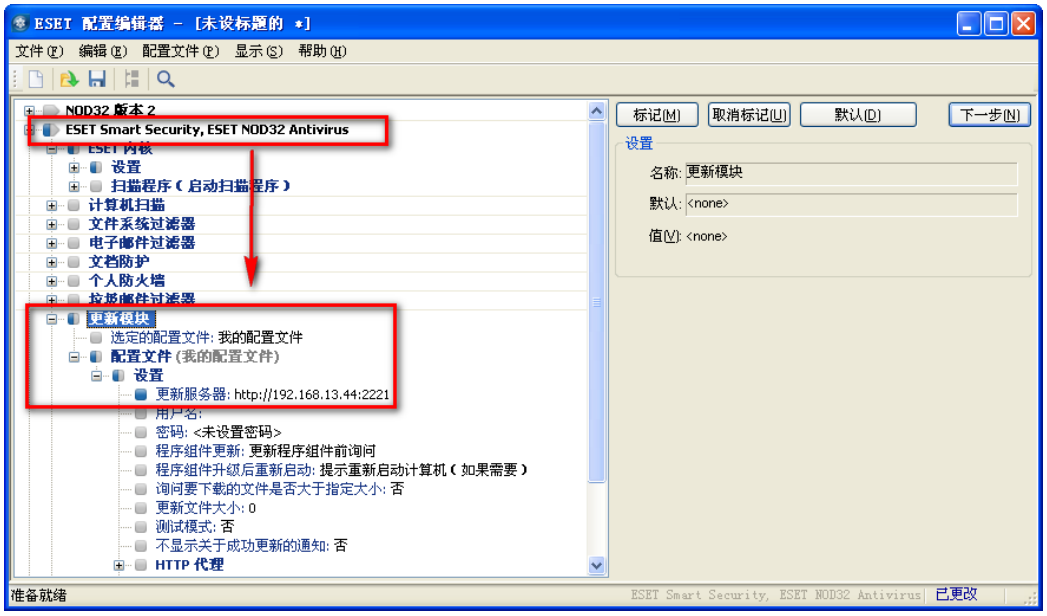


Exclusively Distributed by Version 2 Limited

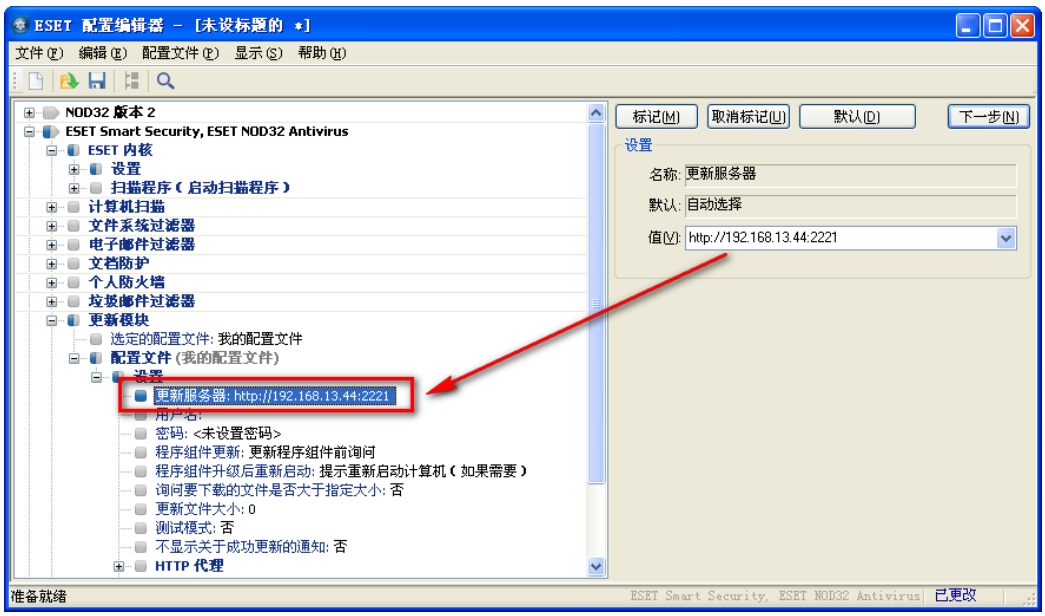


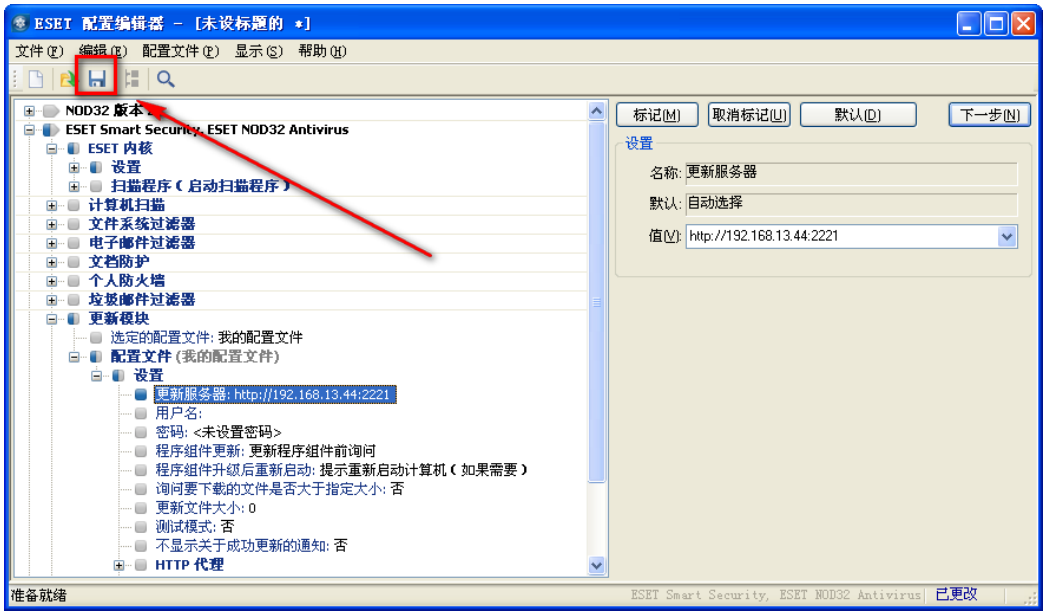
连接到远程管理服务器——是

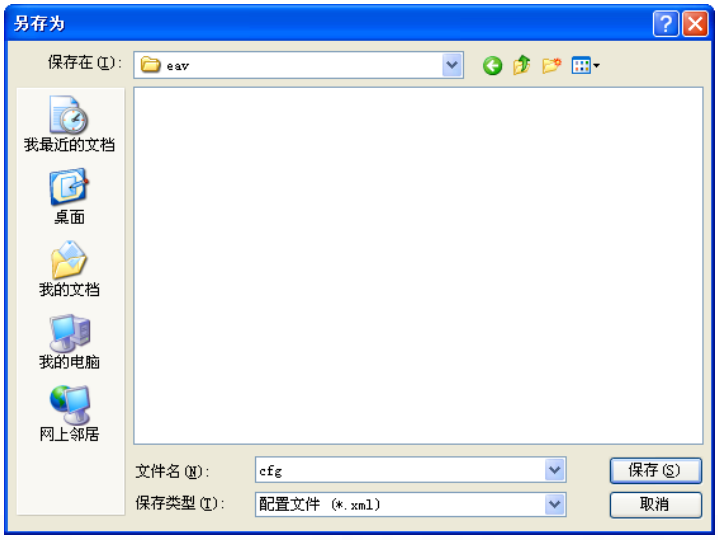
主服务器地址——此处输入服务器 IP 地址



更新服务器地址：http://服务器 IP:2221



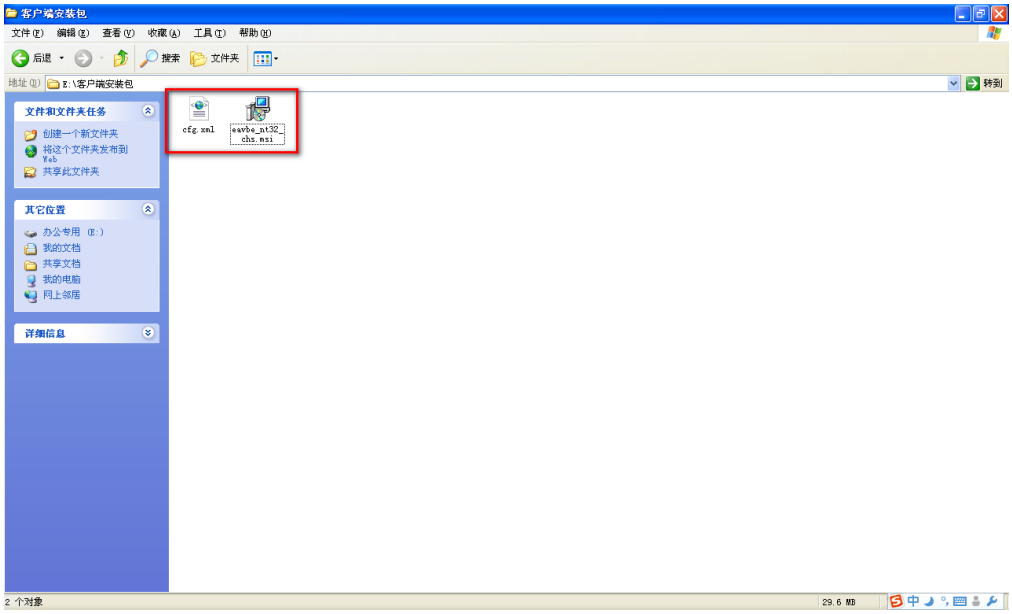


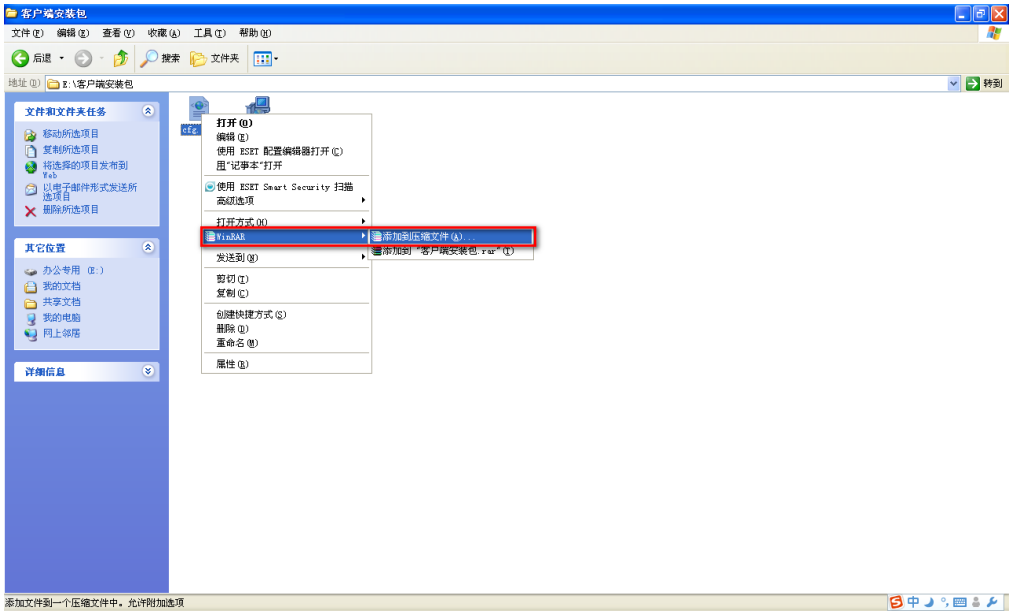


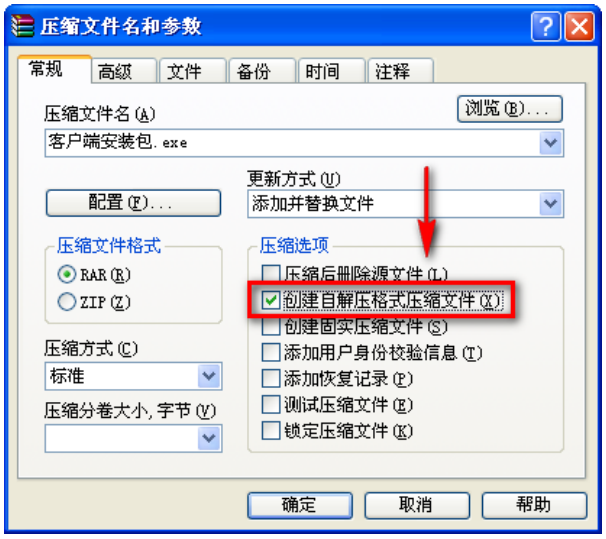
Version 2
Exclusively Distributed by Version 2 Limited

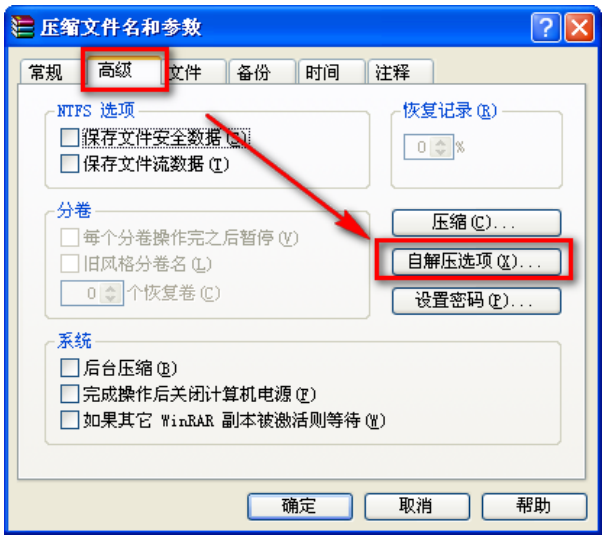
2. 打包客户端

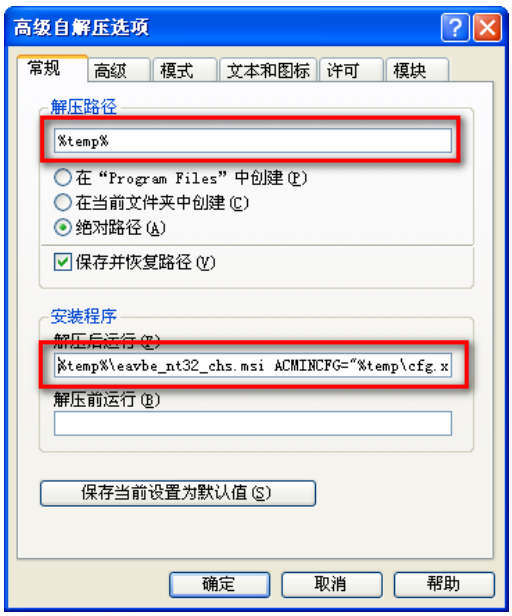
如上图，做好客户端配置文件后，再找到光盘中原始的客户端安装程序进行打包。






压缩文件名和参数
常规
高级
文件
备份
时间
注释
压缩文件名(A)
浏览(B)...
客户端安装包.exe
配置(F)...
更新方式(U)
添加并替换文件
压缩文件格式
RAR(R)
ZIP(Z)
压缩选项
压缩后删除源文件(L)
创建自解压格式压缩文件(X)
创建固实压缩文件(S)
添加用户身份校验信息(T)
添加恢复记录(P)
测试压缩文件(E)
锁定压缩文件(K)
压缩方式(C)
标准
压缩分卷大小,字节(V)
确定
取消
帮助


压缩文件名和参数
常规
高级
文件
备份
时间
注释
NTFS 选项
保存文件安全数据(S)
保存文件流数据(T)
恢复记录(R)
%
分卷
每个分卷操作完之后暂停(V)
旧风格分卷名(L)
个恢复卷(C)
压缩(C)...
自解压选项(X)...
设置密码(P)...
系统
后台压缩(B)
完成操作后关闭计算机电源(F)
如果其它 WinRAR 副本被激活则等待(W)
确定
取消
帮助


高级自解压选项
常规
高级
模式
文本和图标
许可
模块
解压路径
%temp%
在“Program Files”中创建(P)
在当前文件夹中创建(C)
绝对路径(A)
保存并恢复路径(V)
安装程序
解压后运行(E)
%temp%\eavbe_nt32_chs.msi ACMINCFG="%temp\cfg.x
解压前运行(B)
保存当前设置为默认值(S)
确定
取消
帮助

解压路径：%temp%————解压到系统临时文件夹

解压后运行参数：

%temp%\eavbe_nt32_chs.msi ADMINCFG=”%temp%\cfg.xml” /qn REBOOT=”ReallySuppress”

注意其中的分号

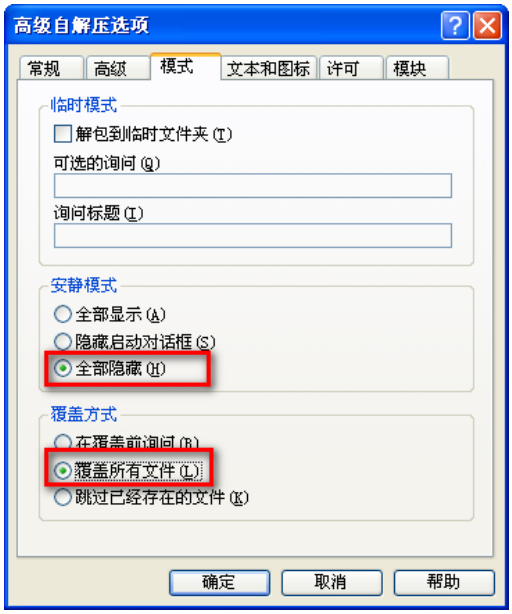
解释：

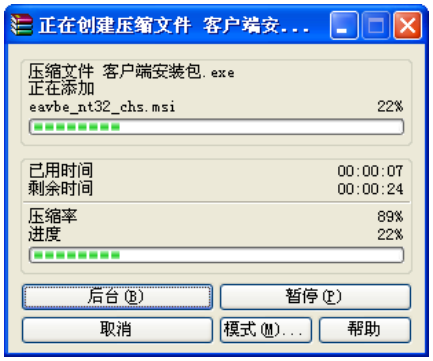
%temp%\eavbe_nt32_chs.msi————解压到系统临时文件夹后，运行程序 eavbe_nt32_chs.msi

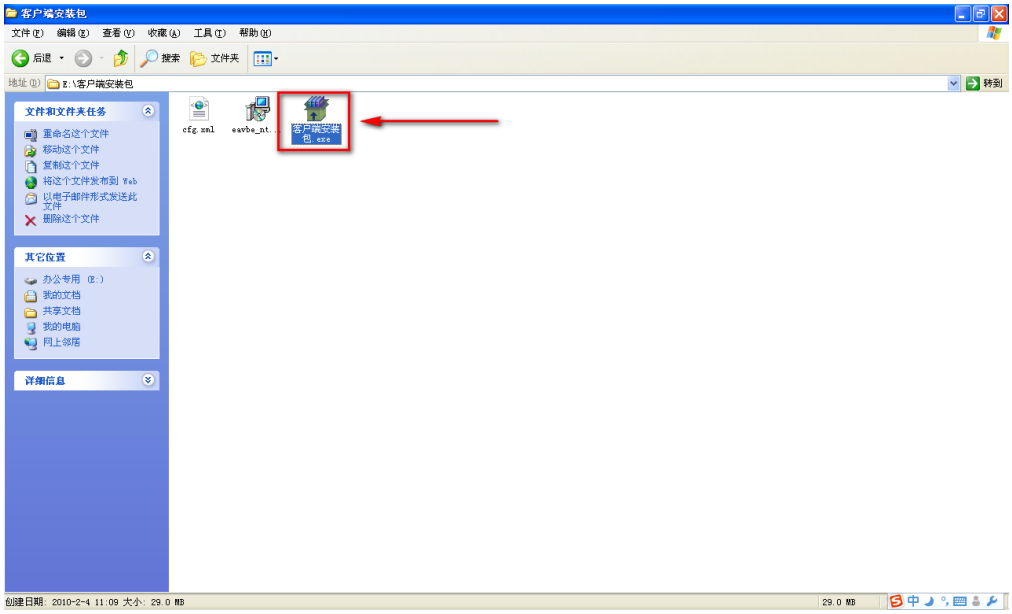
ADMINCFG=”%temp%\cfg.xml”——安装时调用解压到临时文件夹的配置文件 cfg.xml

/qn————————————————静默安装

REBOOT=”ReallySuppress”———— 安装成功后，不重启电脑







经过上述步骤，客户端安装包已经定制好，可以将该安装包通过各种方式发布到 PC 执行安装（例如共享，U 盘拷贝，网页发布等等方法）

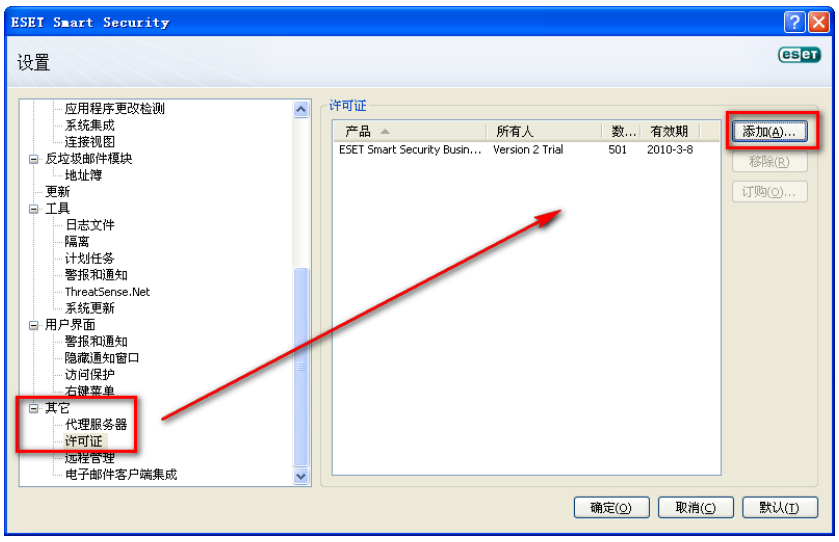
第四章 服务器防病毒软件安装

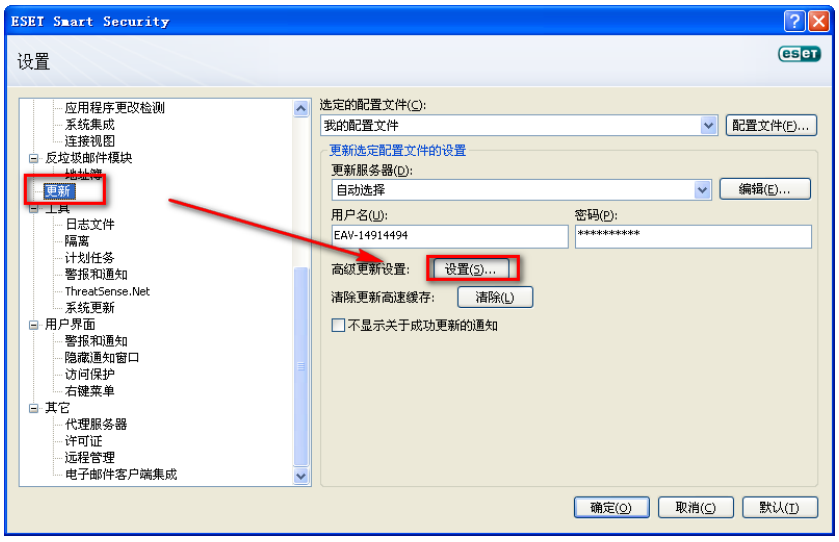
如上图，定制好客户端安装包后，在 ESET NOD32 服务器上，双击该安装包安装杀毒软件。

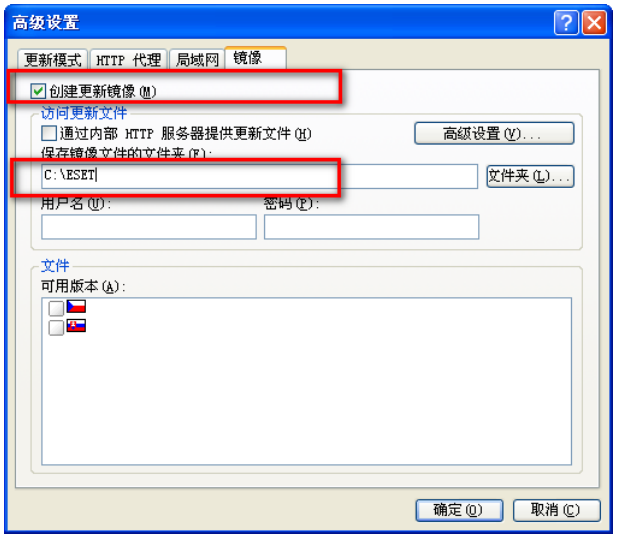
安装程序将依据设定，在后台静默安装，没有图形界面。（备注：系统需启用 windows installer 服务，绝大部分系统都默认启用了）

第五章 使用 IIS 架设本地更新服务器

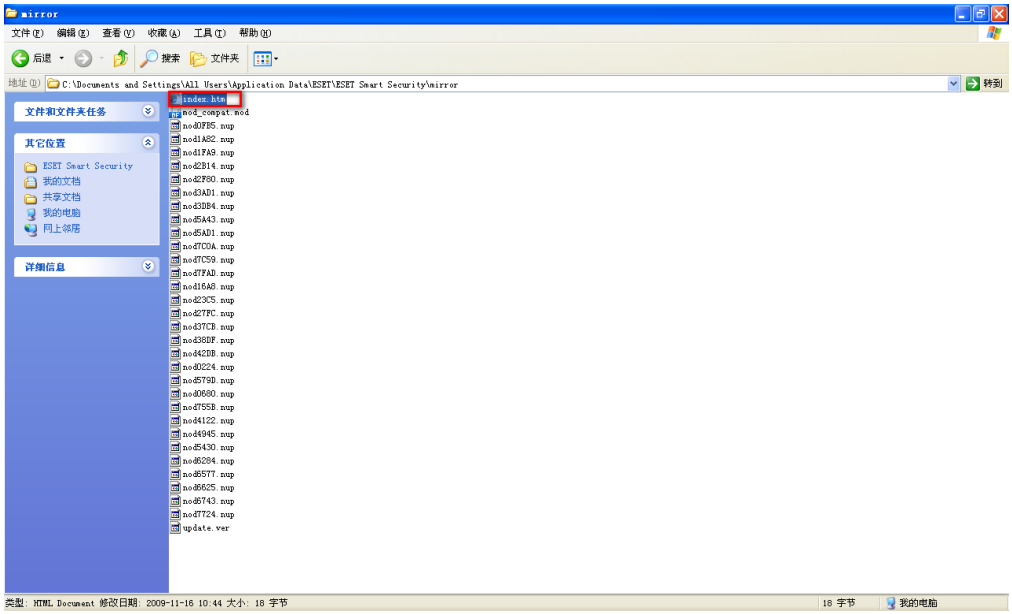
第一步：在服务器上打开 ESET NOD32 程序主界面，然后按键盘的 F5 进入“高级设置”，在选择“其它”—>“许可证”，将企业版的授权许可证导入进去，按确定。再次返回高级设置窗口，选择“更新”->“镜像”标签，然后取消“通过内部 HTTP 服务器提供更新文件”前的对勾，这样 NOD32 将不再利用自己的发布程序来提供更新文件服务。



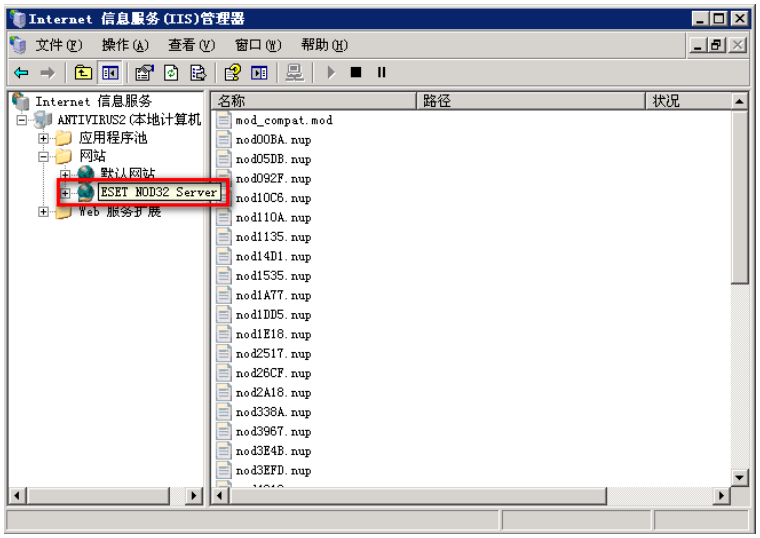


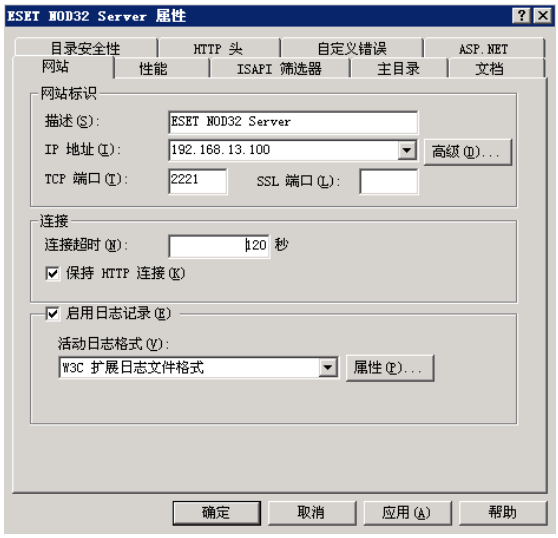


默认情况下 NOD32 网络版升级文件都存储在 C:\Documents and Settings\All Users\Application Data\ESET\ESET Smart Security\mirror 目录下，路径很长，我们可以自己作更改为 C:\ESET，我们变换发布选择 IIS 时也主要针对此目录即可。最好的测试办法就是在该目录下添加一个名为 index.htm 的文件，可以用记事本建立一个 TXT 文本文件输入几个字符，然后将其名称与后缀名强行修改为 index.htm 并保存退出。



第二布：接下来启动服务器上的 IIS，然后通过“新建网站”建立一个站点，这个站点的主目录就是上文提到的 C:\ ESET\目录。同时 TCP 发布端口也要与之前配置的终端升级端口相符，一般默认端口为 2221（具体数字可以到服务器 NOD32 的“通过内部 HTTP 服务器提供更新文件”->“高级设置”查询）

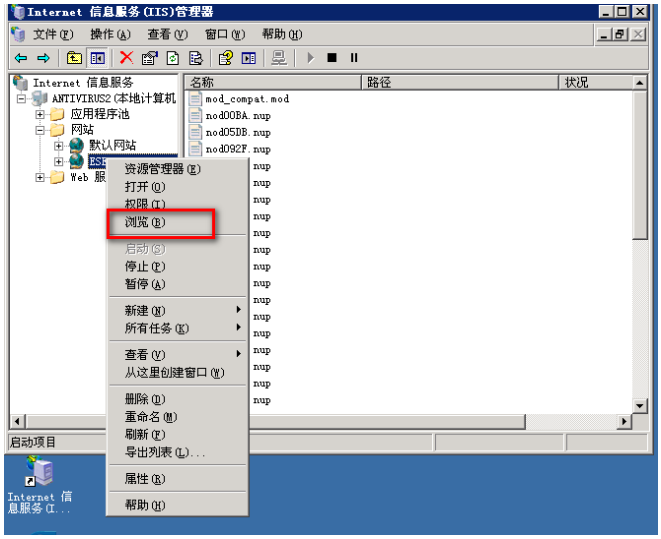




第四步：发布主目录标签下选择“读取”权限即可，不需要给予写入或目录浏览等权限，否则容易带来安全问题。

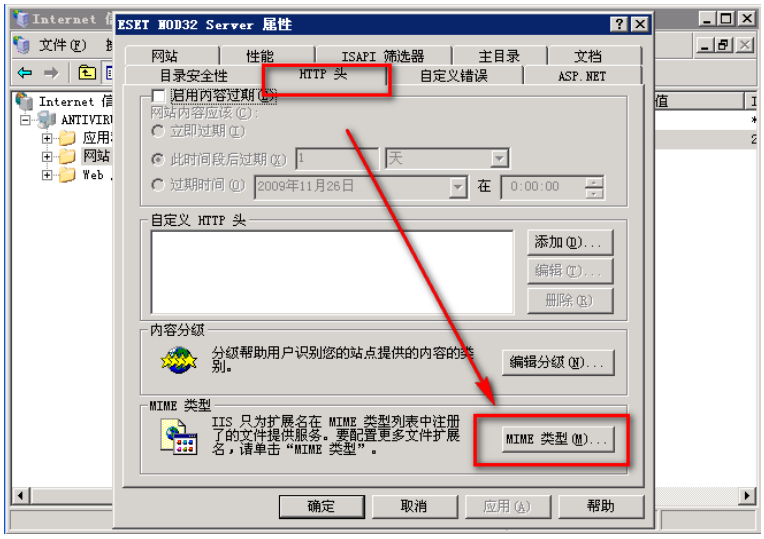
注意下图路径中的本地路径：C:\ESET

第五步：发布完毕后我们进行调试，选择“浏览”网站如果可以看到 index.htm 文件中填写的文本内容即可。

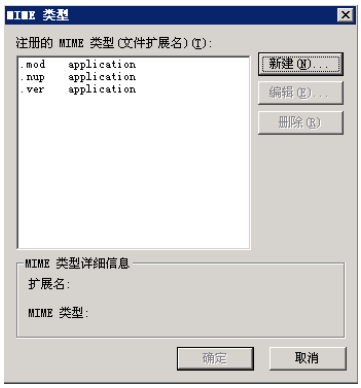


第六步：我们可以在终端计算机上通过"http://服务器地址:发布端口"来访问，如果也能够看到 index.htm 文件中填写的文本内容就说明发布工作彻底成功了。不过我们还需要针对 IIS 发布文件的 MIME 类型进行配置，如果不配置终端升级病毒库时会出现“找不到升级文件”的错误提示。在服务器 IIS 管理器中选择“HTTP 头”标签，然后点“MIME 类型”按钮。

Exclusively Distributed by Version 2 Limited



第七步：在 MIME 类型窗口中通过新建建立三个 MIME 文件扩展条目，第一个扩展名是.nup，类型是 application；第二个扩展名是.ver，MIME 类型是 application；第三个扩展名是.mod，MIME 类型是 application。建立完毕后确定即可。



第八步：添加 MIME 类型后我们的终端就可以顺利更新了。实际上这是因为默认情况下 IIS 无法识别.nup 与.ver 和.mod 升级文件，默认并不容易他们被 IIS 来宾所访问，添加 MIME 后上述问题解决，终端计算机才可以顺利的通过 WWW 服务获取.nup 与.ver 和.mod 升级文件，从而顺利的更新病毒库升级问。

Exclusively Distributed by Version 2 Limited

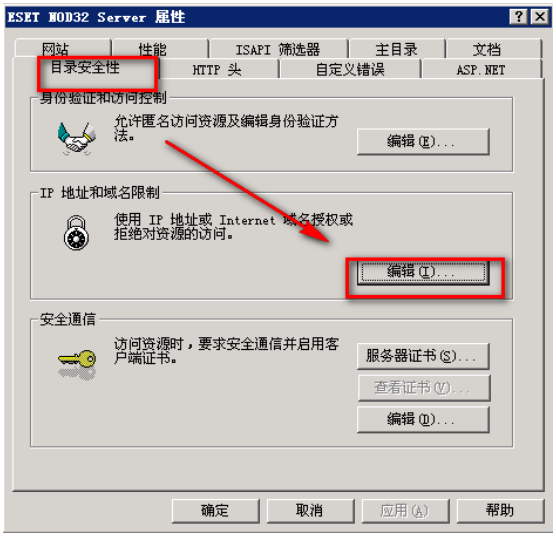
第六章 IIS 高级功能

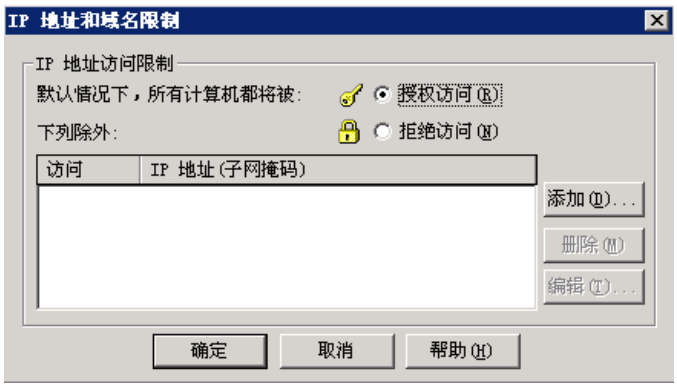
备注：此部分为可选内容

在经过上面的基本设置后，ESET NOD32 的客户端就可以连接到服务器升级病毒库了，如果我们还需要一些更加高级的设置，例如设置客户端连接到服务器升级需要用户名和密码、仅仅允许某个网段内的机器升级病毒库等等，则需要参照如下部分：

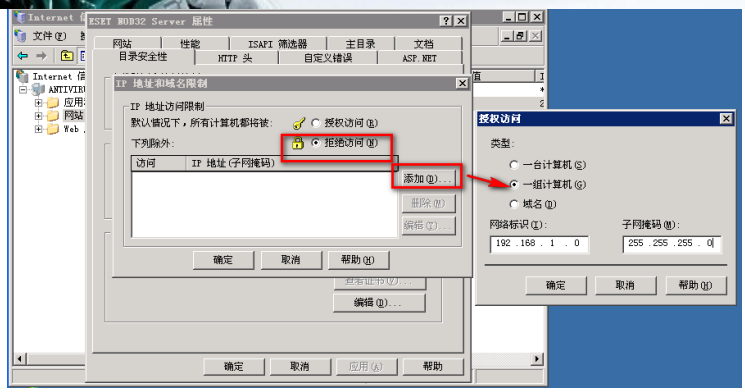
（1）针对 IP 地址进行管理与控制：

第一步：我们依旧按照上文所说的方法通过 IIS 来发布病毒库更新文件，接下来在对应的发布站点属性窗口中选择“目录安全性”，然后点 IP 地址和域名限制右下角的“编辑”按钮，在这里我们可以针对访问该站点（病毒库升级文件）的源 IP 地址范围进行限制，例如设置默认情况下所有计算机都将被“拒绝访问”，同时“添加”某个网段计算机的授权访问。





第二步：添加过程中是支持针对网段进行管理与控制的，例如选择只容许 192.168.1.0　255.255.255.0 这个网段的主机通过本服务器进行 NOD32 病毒库升级。



第三步：确认完毕后最终效果就是默认情况下所有计算机都将被拒绝访问本服务器发布的病毒库文件升级目录，除了 192.168.1.0 255.255.255.0 这个网段内的主机可以顺利升级。

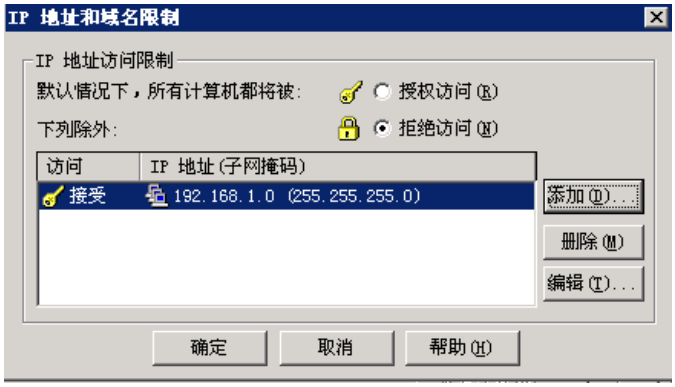


图 11

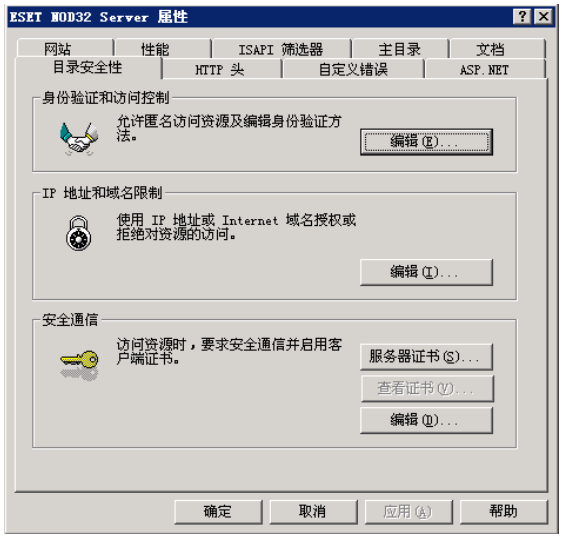
第四步：这样当源地址不是合法 IP 段的 NOD32 终端机升级病毒库时，即使服务器地址，端口等信息填写正确，在升级时也会出现“病毒库无法更新，未经授权的访问”这个错误提示，从而最大限度的解决了非授权终端的非法升级问题。

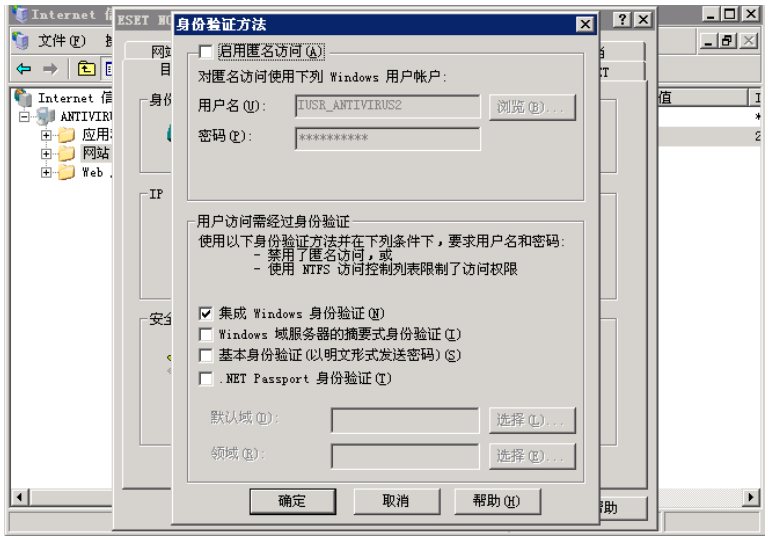
（2）针对用户名和密码进行管理与控制：

上文介绍的通过地址进行限制固然是个好办法，但是在实际中可能服务器地址被公开，如果不设置用户名和密码，则任何知道服务器 IP 的人都可以连接到服务器升级病毒库，解决的方法就是通过 IIS 的帐户验证功能我们可以实现只有知道了合法的用户名和密码的终端才能够顺利的通过内网同步更新服务器来升级病毒库。具体操作如下。

第一步：我们继续打开 IIS 发布的 NOD32 病毒库升级站点的“属性”窗口，选择“目录安全性”标签，然后点身份验证和访问控制旁边的“编辑”按钮，将默认的“启用匿名访问”前的对勾去掉。

Exclusively Distributed by Version 2 Limited





第二步：在用户访问需经过身份验证处选择“集成身份验证”。然后确定。

第三步：接下来建立一个具备一定权限的系统帐户，当然不推荐使用“管理员权限”，选择 C:\ESET 目录，设置其“安全属性”，添加该帐户对镜像文件夹目录有“读取和运行，列出文件夹目录，读取”权限。

第四步：确定后我们在终端上升级病毒库时就需要身份验证了，必须输入了与之前添加的系统帐户一致的信息才能够实现更新功能。例如笔者之前添加的系统帐户是 antivirusserver，密码为 111111。那么添加后终端升级时出现的“许可证详细信息”窗口中也要填写用户名 antivirusserver，密码 111111。

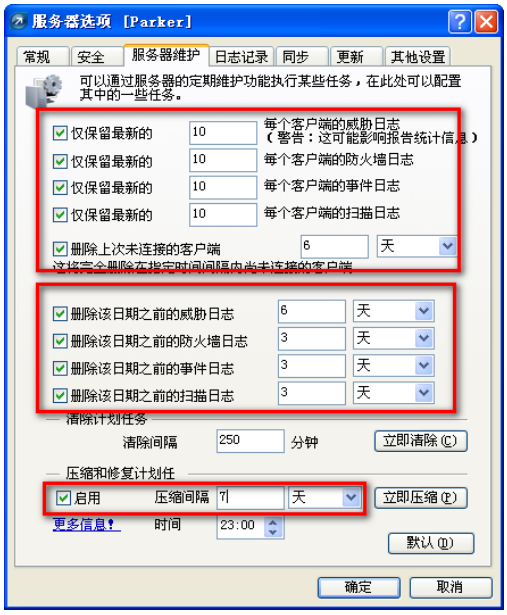
Version 2 二版 www.version-2.com
Exclusively Distributed by Version 2 Limited

第五步：输入正确的身份验证信息后终端 NOD32 才能够顺利更新病毒库文件。

第七章 服务器自动维护

由于客户端数量非常多，客户端的任何异常信息都将记录到远程管理服务器中，为了服务器运行的稳定，建议设置服务器自动维护。

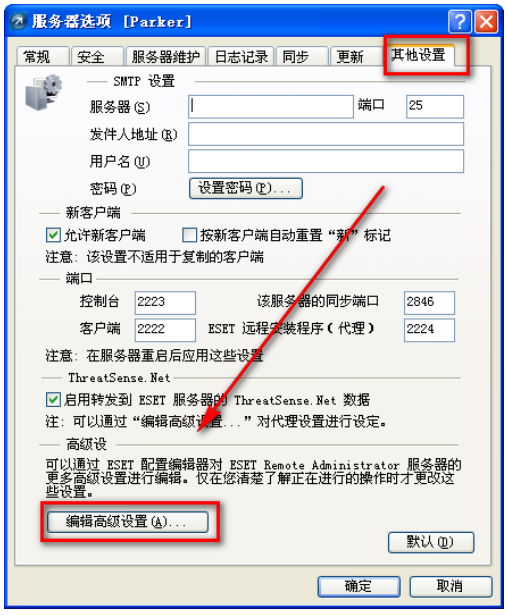
打开控制台——服务器选项，如下图：

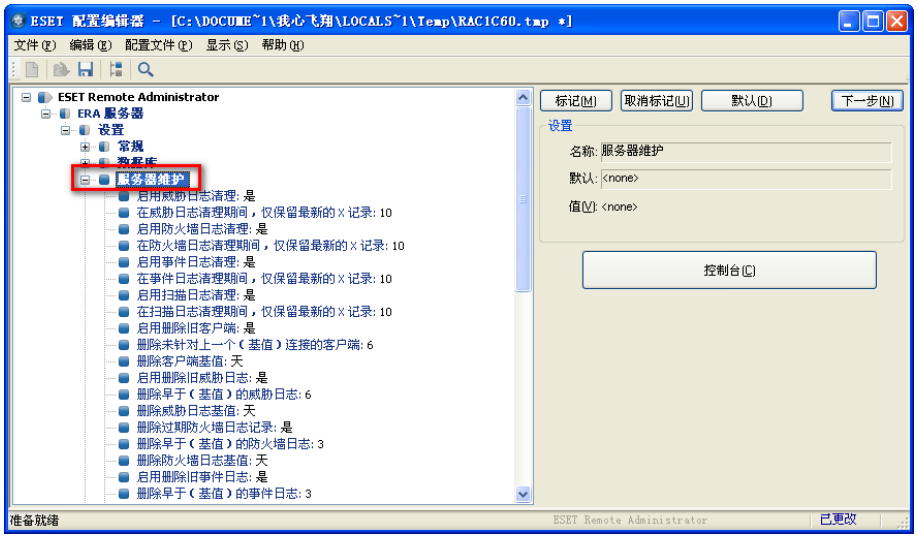


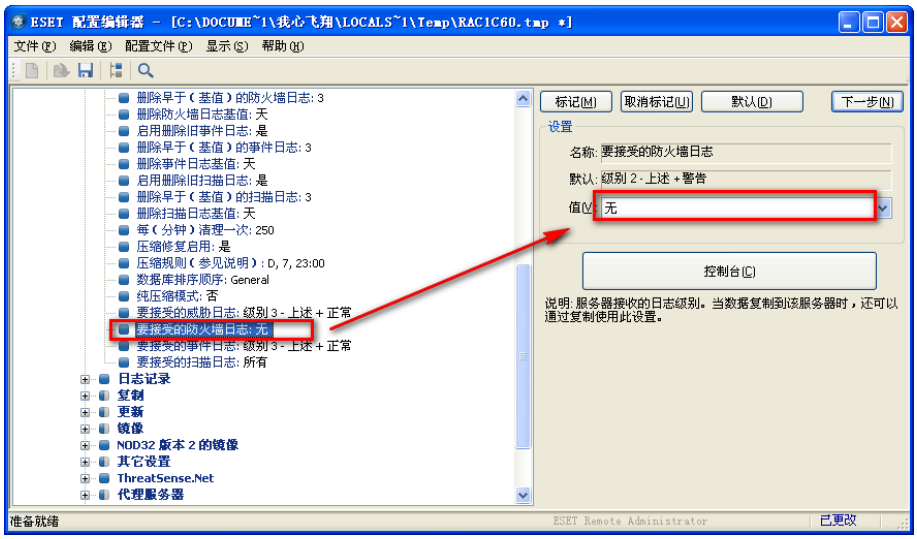
如果您安装的是 ESET NOD32 安全套装企业版，需要作如下设置，如果是 ESET NOD32 防病毒软件企业版，则可以略过此步骤。

打开“服务器选项”——“其他设置”，设置 ERA 服务器不接受防火墙日志。

原因：防火墙日志非常之多，大型网络中数据库增量很快，建议不记录防火墙日志。







到此 ESET NOD32 企业版已经部署完成。

Version 2 二版 www.version-2.com
Exclusively Distributed by Version 2 Limited

第八章 服务与支持

尊敬的用户，非常感谢您选购 ESET NOD32 企业版，以下是 ESET NOD32 售后服务承诺函：

服务内容：

在使用年限内，免费提供防病毒软件程序升级及技术服务；

技术支持响应时间保证：

对于日常技术支持咨询邮件，将在半小时内予以答复。

对于日常电话咨询，全部人工当场解答，不通过电脑自动应答。

对提交的可疑文件（包括新病毒），二版科技(深圳)有限公司在接到可疑文件的 24 小时内给予答复。

紧急情况下，如可疑病毒开始在系统内大量扩散，二版科技(深圳)有限公司会在收到可疑程序后一小时内向用户提供紧急应对方法。

在接到用户提出的问题后，二版科技(深圳)有限公司将跟据问题的种类和紧急程度以及先后顺序，保证在规定时间内向用户作出响应和提供相应的支持。问题种类和响应级别参照下表。

严重性		定义	反应时间	问题解决时间
A	最高级 Critical	软件死锁、没有反应。 病毒爆发、大量扩散。	30 分钟	1 个工作日
B	紧急 Urgent	系统主要功能无法执行。 系统性能突然严重降低。	4 小时	2 个工作日
C	重要 Important	系统出现错误，不过有变通方法可以暂时运作。 系统出现细微错误，不影响日常正常作业。 一般性的产品使用问题。	1 个工作天	3 个工作日
D	普通 Normal	索取产品更新（非电子数据方式）。 索取一般信息。	1 个工作天	3 - 5 个工作日

注：以上解决问题的时间，是基于用户的良好配合

防病毒软件的更新：

在服务期内，为用户提供免费的病毒库更新服务和产品升级服务。

免费紧急事件响应：

发生紧急事件（病毒爆发）时，用户应立即通知二版科技(深圳)有限公司，二版科技(深圳)有限公司应了解病毒爆发状况，如病毒爆发地点、病毒感染现象等确定参与紧急事件响应技术人员和响应方式。

如果出现的紧急情况需要现场支持，二版科技(深圳)有限公司将提供现场支持服务，响应时间参照响应条例并加上路途所需时间。

对于出现的紧急情况，二版科技(深圳)有限公司将以最有效的方式处理出现的问题，并不限于用户所使用的产品，确保将损失降低到最低程度。

通过通讯方式提供技术服务

在服务期间内，二版科技(深圳)有限公司承诺免费为用户提供计算机病毒防治技术咨询服务。服务方式可通过电话、电子邮件、传真等。

电话：0755-83015850

传真：0755-83015890

电邮：support@version-2.com.cn